# BUNDESREPUBLIK DEUTSCHLAND

**PRIORITY DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

4

## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

| | |
|---|---|
| **Aktenzeichen:** | 199 28 343.5 |
| **Anmeldetag:** | 21. Juni 1999 |
| **Anmelder/Inhaber:** | DeTeMobil Deutsche Telekom MobilNet GmbH, Bonn/DE |
| **Bezeichnung:** | System und Verfahren zum vereinfachten Zugang zu Telekommunikationsnetzen und zur Abrechnung von Telekommunikationsdienstleistungen |
| **IPC:** | H 04 M, H 04 Q |

**Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.**

München, den 31. August 2000
**Deutsches Patent- und Markenamt**
**Der Präsident**
Im Auftrag

Agurks

A 9161
06/00
EDV-L

DeTeMobil Deutsche Telekom MobilNet GmbH

# System und Verfahren zum vereinfachten Zugang zu Telekommunikationsnetzen und zur Abrechnung von Telekommunikationsdienstleistungen

## Einleitung

Die im Folgenden beschriebene Idee stellt den klassischen Mechanismen von Netzbetreibern (i.d.R. Mobilfunk), ihren Kunden Dienstleistungen zur Verfügung zu stellen und für die Bereitstellung derselbigen Entgelte zu nehmen, neue Prozesse entgegen. Es geht in diesem Zusammenhang primär um neue Zugangsmechanismen und -medien zum (mobilen) Telekommunikationsnetz, veränderte Sicherheitsmechanismen sowie um innovative Zahlverfahren. Der Vereinfachung halber wird die Erfindungsidee im Folgenden anhand von Mobilfunknetzen des GSM-Standards beschrieben, ist jedoch auch auf andere Telekommunikationsnetze anwendbar, soweit die in der Beschreibung gemachten Randbedingungen auch auf diese Netze anwendbar sind.

## Der klassische Ansatz/Status quo

Allgemein kann gesagt werden, dass ein Mobilfunkbetreiber mittels seines Telekommunikationsnetzes eine Infrastruktur bereitstellt, die die Nutzung bestimmter Dienstleistungen (primär Telefonie) ermöglicht. Diese Dienstleistungen können von beliebigen Teilnehmern unter der Erfüllung gewisser

Randbedingungen gegen Entgelt genutzt werden. Der Netzbetreiber entscheidet in jedem einzelnen Fall, welchem Teilnehmer er den Zugang zu seinem Telekommunikationsnetz (und damit zu seinen Diensten) erlaubt und welchen er von der Inanspruchnahme der mit dem Zugang verbundenen Dienstleistungen ausschließt. Im klassischen Fall gibt es zwei Ansätze die einem Teilnehmer eine Zugangsberechtigung zu einem Telekommunikationsnetz erlauben:

a) auf Subskriptionsbasis:
Der Teilnehmer schließt einen Vertrag mit dem Netzbetreiber (Home Operator) ab, der dem Teilnehmer für die Vertragslaufzeit die Nutzung bestimmter Dienstleistungen ermöglicht. Typisch für diesen Ansatz ist, dass der Nutzer i.d.R. einen kontinuierlichen Grundbetrag und für die Inanspruchnahme von Dienstleistungen ein mengenabhängiges Entgelt entrichtet. Die Bezahlung erfolgt i.d.R. auf kreditorischer Basis per (Monats-)Rechnung.

b auf Prepaidbasis:
Der Teilnehmer kauft beim Home Operator eine bestimmte Art und Menge an Dienstleistungen ein und bezahlt diese im Voraus. Dafür steht ihm die Nutzung des Netzes und der jeweiligen Dienstleistungen bis zu dem vereinbarten, eingekauften Umfang zu. Der Netzbetreiber überprüft die Art und Menge der genutzten Dienste und entzieht dem Teilnehmer nach Verbrauch seines eingekauften Kontingents wieder die Zugangsberechtigung.

Speziell für GSM-Mobilfunknetze existieren für die Nutzung von Telekommunikationsdiensten zwei Varianten:

a) Der Teilnehmer nutzt ausschließlich die Infrastruktur des Home Operators. Das Entgelt für die Nutzung wird nach einem der obigen Verfahren entrichtet.

b) Der Teilnehmer nutzt zumindest teilweise die Infrastruktur eines anderen (visited) Operators. Das Entgelt wird an den Home Operator nach obigen Verfahren entrichtet. Darüber hinaus werden, ohne Einflußnahme des Teilnehmers, für die Inanspruchnahme des Fremdnetzes entsprechende Ausgleichszahlungen zwischen den Operatoren geleistet (Roaming Fall).

Die beschriebenen Ansätze machen deutlich, dass die Kontrolle des Netzbetreibers über die Zugangsberechtigung des Teilnehmers eine zentrale Funktion darstellt. Sowohl im Fall der ausschließlichen Nutzung des Home Netzes als auch im Roaming Fall sind für GSM Mechanismen definiert, die die Identität und Authentizität des Teilnehmers sicherstellen. Das technisches Medium, welches dieses ermöglicht, ist die Chipkarte (SIM) in Kombination mit Daten im Netz (z.B. HLR/AC, VLR). Letztendlich stellt die SIM die Basis dar, die es dem Operator (Home oder Visited) erlaubt, die Zugangsberechtigung des Teilnehmers zu überprüfen. Der folgende Ansatz nimmt teilweise von diesem Paradigma Abstand.

**Innovativer Ansatz**

Der klassische Ansatz stellt über die beschriebenen Mechanismen im Grunde 2 Sachen sicher:

a) Der Netzbetreiber weiß, wer der Teilnehmer ist.

b) Der Netzbetreiber weiß, dass und wie er das Entgelt für die in Anspruch genommene Dienstleistung bekommt (oder schon bekommen hat).

Noch substantieller betrachtet ist eigentlich nur der Punkt b) entscheidend. Deshalb wird in dem folgenden Ansatz eine Alternative aufgezeigt, die letzteres sicherstellt, jedoch den klassischen Ansatz verläßt.

Bei diesem Ansatz gilt wie im klassischen Fall:

- der Netzbetreiber stellt eine Infrastruktur und Dienste bereit;
- gegen Entgelt können diese genutzt werden;
- der Netzbetreiber kontrolliert den Zugang zu seinen Diensten.

Zu den beiden obigen Varianten, über die a) Subscription oder b) Prepaid die Zugangsberechtigung zum Netz zu erhalten, wird nun jedoch folgende Forderung aufgestellt:

c) Der Teilnehmer kann im Voraus (oder im Nachhinein) dem Netzbetreiber auf irgendeine Art und Weise nachweisen (oder überzeugen), dass eine Bezahlung der in Anspruch genommenen (oder zu nehmenden) Dienstleistung geleistet wird (oder bereits geleistet wurde), indem er z.B.
   1) zweifelsfrei seine Identität und eine damit verbundene Verläßlichkeit nachweist (z.B. "Ich bin der Bundeskanzler der Bundesrepublik Deutschland"), z.B. durch eine digitale Signatur;
   2) direkt über vertrauensvolle Mechanismen bezahlt (EC-Karte, Elektronische Börse)
   3) zweifelsfrei seine Verbundenheit zu einer vertraulichen, dritten Partei nachweist, die für die Bezahlung einsteht (Kreditkartenorganisation).

Kann der Teilnehmer eine der oben genannten Ansprüche erfüllen, so ist primär dem Anspruch des Netzbetreibers, ein Entgelt vom Teilnehmer zu erhalten, genüge getan - je nach

realsiertem Verfahren und Prozessumfeld ist sogar der Punkt "Wer ist der Teilnehmer?" zu erfüllen, was allerdings nicht zwingend erforderlich ist.

Je nach Ausprägung und Realisierungsvariante sind die Ansprüche des Netzbetreibers bzgl. der Bezahlsicherheit des Teilnehmers sicherlich unterschiedlich, auch im Vergleich zum klassischen Ansatz. Das Maß an Sicherheit liegt allerdings alleine im Ermessen des Netzbetreibers. Zur Verdeutlichung dieser Tatsache dient der klassische Ansatz im GSM Netz, wo der Netzbetreiber

- über die technische Sicherheit der SIM entscheidet;
- frei über den Authentikationsalgorithmus entscheidet (auch die Auswahl eines einfachen "XOR-Algorithmus" wäre erlaubt);
- die individuellen Teilnehmer Keys (Ki) selbst bestimmt (auch ein konstanter Schlüssel für alle seine Teilnehmer wäre erlaubt);
- entscheidet über das Sicherheitslevel des gesamten Schlüsselmanagementprozesses (Generierung, Transport, Speicherung).

Als Folge der Tatsache, dass der Netzbetreiber die "Sicherheitshoheit" über seinen Identifikations- und Authentikationsprozess besitzt, wird im folgenden eine spezielle Ausprägung des Ansatzes aufgezeigt.

**Inanspruchnahme von Telekommunikationsdienstleistungen mittels Kreditkarten**

Bisherige Anwendungen, die den Einsatz von Kreditkarten als Bezahlmedium in Telekommunikationsnetzen beschreiben, setzen

alle voraus, dass der Teilnehmer eine prinzipielle Zugangsberechtigung zu einem Telekommunikationsnetz besitzt, die er vorab bereits durch eine der obigen Varianten (Subscription, Prepaid) erworben hat. Das Bezahlen per Kreditkarte ist in diesen Fällen als Methode anzusehen, wo Dienstleistungen (vorwiegend dritter Parteien) auf diesem Weg (eben über die Kreditkarte) abgerechnet werden. Dabei gibt es eine Bandbreite an Realiserungsmöglichkeiten, die sich in Sicherheit und Benutzerfreundlichkeit unterscheiden. Beispielsweise seien die folgenden Varianten genannt:

- der Teilnehmer nennt einem Sprachserver seine Kreditkartennummer;
- er verwendet die Tastatur (DTMF-Töne) zur Eingabe seiner Kreditkartennummer;
- er verschickt eine SMS an einen speziellen Server mit seinen Kreditkartendaten;
- anhand seiner MSISDN oder IMSI wird eine Zuordnung zu seiner Kreditkarte hergestellt (die der Teilnehmer vorab dem Netzbetreiber bekannt gemacht hat).

Neu an dem hier beschriebenen Verfahren ist, dass einem Teilnehmer die Inanspruchnahme von Telekommunikationsdienstleistungen auch ohne gültige (klassische) Zugangsberechtigung ermöglicht wird. Praktisch heißt dies, dass auch ohne gültige SIM dem Teilnehmer eine Dienstenutzung ermöglicht wird. Technisch wird dabei an der Stelle eingegriffen, wo im klassischen Fall die Identifikations- und Authentitikationsprozeduren des Netzbetreibers einsetzen.

Nehme man als Beispiel den Fall, dass eine ungültige SIM im Endgerät verwendet wird und damit versucht wird, sich Zugang

zu einem GSM-Netz zu verschaffen. Ungültige SIM heißt in diesem Zusammenhang:

- nicht registriert (dem Home Operator unbekannte IMSI)
- nicht Roaming-fähig (die IMSI gehört einem Home Operator, der dem Teilnehmer keine Roaming Erlaubnis erteilt hat)
- nicht authentisch (die Authentikationsprozedur scheitert, z.B. wegen falschem Ki)

In allen Fällen schickt im klassischen Fall der Netzbetreiber dem Endgerät eine entsprechende Fehlermeldung und verweigert den Zugang zu seiner Infrastruktur (eine Ausnahme bildet lediglich der Notruf "112").

Der neue Ansatz ändert das bisherige Verfahren insofern ab, dass der Netzbetreiber zwar registriert, dass die verwendete SIM keine Zugangsberechtigung im klassischen Sinn besitzt, er dem Teilnehmer jedoch nicht prinzipiell den Zugang verweigert. Vielmehr bietet der Netzbetreiber dem Teilnehmer mittels geeigneter, zu definierender Prozeduren an, sich alternativ über seine Kreditkarte zu identifizieren. Ist die Identifikation im Sinne des Netzbetreibers erfolgreich, so bietet dieser dem Teilnehmer ein gewisses Spektrum an Diensten an. Eine gewisse "Bezahlgarantie" erreicht der Netzbetreiber einerseits durch die Sicherheit des definierten Identifikationsmechanismus wie auch durch die üblichen Bezahlgarantien von Kreditkartenfirmen bei Inanspruchnahme von Dienstleistungen ihrer Kunden.

Beim Identifikationsprozess über die Kreditkarte sind wiederum verschiedene Varianten denkbar:

a) Der (im Telekommunikationsnetz nicht registrierte) Teilnehmer erhält Zugang nur zu einem bestimmten Ziel

(evtl. mittels jeder beliebigen Rufnummer), unter dem er sich mittels Eingabe seiner Kreditkartennummer identifizieren kann (i.d.R auf "per Call Basis"). Dies kann gewisse Plausibilitäts- und Sicherheitchecks mit einschließen, wie z.B. Passwortschutz, die Eingabe zusätzlicher persönlicher Daten, online-check der Daten bei der Kreditkartenorganisation etc..

b) Der Teilnehmer erhält das Recht auf abgehende Kurznachrichten und kann sich in ähnlicher Weise wie unter a) registrieren.

c) Für den Fall, dass die Kreditkarte chipkartenbasiert ist, übermittelt der Teilnehmer seine Kreditkartendaten elektronisch, also direkt mit seiner Kreditkarte. Dies kann auf verschiedene Weise geschehen:

- das Endgerät erlaubt einen Zugriff auf einen zweiten Kartenleser, in dem die Kreditkarte des Teilnehmers steckt
- das Endgerät akzeptiert die Kreditkarte anstelle der SIM. Anstatt der IMSI (wie in GSM) wird die Kreditkartennummer ganz oder teilweise bei der Registrierungsprozedur an das Netz geschickt. Der Netzbetreiber muß dabei in der Lage sein, diesen Fall von der klassischen Registrierungsprozedur zu unterscheiden.

d) Der Netzbetreiber kann selbst eine Zuordnung zwischen der (nicht im klassischen Sinn registrierten) SIM zu einer Kreditkarte vornehmen. Dies bedarf einer vorherigen, einmaligen Prozedur, bei der diese Zuordnung hergestellt wird.

**Technische Realisierung**

Um nicht telefonierfähigen (im klassischen Sinne) Teilnehmern eine Dienstleistung (i.d.R. Telefonie) zu ermöglichen, sind je nach Ausprägung des Ansatzes bestimmte Systenvoraussetzungen zu schaffen (hier am Beispiel GSM), die die folgenden Forderungen erfüllen:

- einem nicht roamingfähigen oder nicht registrierten oder nicht authentischem Teilnehmer ist ein Zugang zum Telekommunikationsnetz zu gewähren
- der Zugang erlaubt nur eingeschränkte Funktionalität (z.B. nur abgehende Calls (MoC)) zu einem bestimmeten Ziel
- über den Zugang wird ein Bezahlverfahren mittels Kreditkarte bereitgestellt
- eine über die Kreditkarte vorgenommene, sichere Identifizierung des Teilnehmers erlaubt ihm die eingeschränkte Nutzung des Netzes (z.B. MoCs)
- die Abrechnung der Dienstleistung basiert auf der Nutzung der Kreditkarte (z.B. auf dem Kreditkartenkonto)

Die folgenden Abbildungen 1 und 2 zeigen eine Implementierungsvariante, die diesen Forderungen gerecht wird. Abbildung 1 zeigt die Einbuchprozedur und die damit verbundenen Systemanpassungen und Abbildung 2 beschreibt den Identifikationsprozess mittels Kreditkarte.

**Weitere technische Variante**

Eine spezielle Ausprägung dieses Ansatzes verwendet als Zugangsmedium zum GSM-Netz eine Chipkarte, die im GSM-Netz des Home-Operators zwar registriert ist, jedoch mit deutlich verringerter Funktionalität (Simple-SIM). So muß zwar das zur Registrierung verwendete Simple-HLR (s. Abb. 3) gewisse Funktionalitäten (insbesondere auf seinen Schnittstellen) besitzen, kann intern jedoch deutlich einfacher implementiert sein (z.B. nur ein Standardprofil, keine MSISDNs, vereinfachte Authentikationsmechanismen etc.). Auch die verwendete Chipkarte kann in seiner Funktionalität deutlich zur Standard-SIM (nach TS GSM 11.11) reduziert sein. Selbst ein Ansatz, eine chipkartenbasierte Kreditkarte direkt als Zugangsmedium einzusetzen, ist unter der Voraussetzung, dass das verwendete Endgerät dies unterstützt, denkbar.

Zusammenfassend einige wichtige technische Charakteristika :

- Ein Spezialmodul im VLR sorgt dafür, dass die Error-Meldungen des HLR entsprechend ausgewertet und umgesetzt werden. So wird z.B. eine ODB-Sperre eingerichtet, alternative ein IN-Flag gesetzt und Authentikation und Ciphering abgeschaltet
- Bei der Verwendung von ODB-Flags wird nachfolgend auf die Identifizierung per Kreditkartekarte die Zielrufnummer nachgewählt und der Ruf aufgebaut. Bei der Verwendung eines IN-Triggers kann schon bei Anwahl des CC-Servers die Zielrufnummer angewählt werden
- Bei Verwendung von Simple-SIMs kann die vereinfachte Authentikation mit konstanten, einheitlichen Challenge/Response-Paaren durchgeführt werden oder mit

variablen Challenge/Response-Paaren, die durch kryptographische Verfahren im SIMPLE-HLR erzeugt werden.

5

Einbuchen ins GSM-Netz

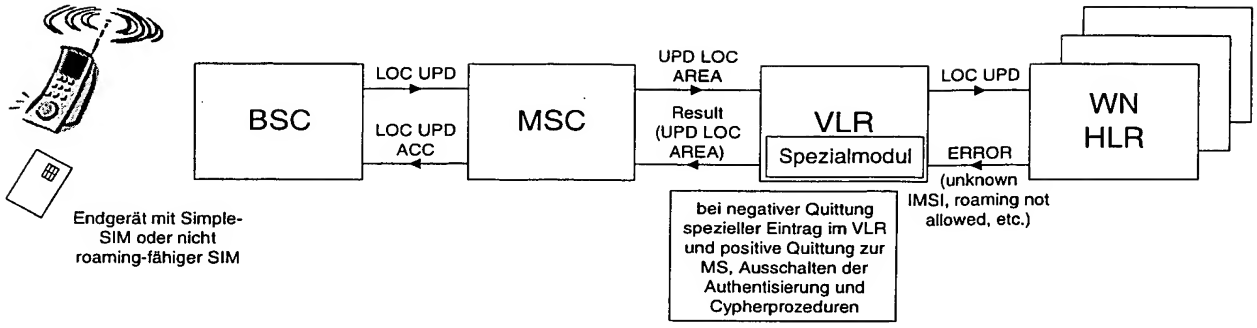
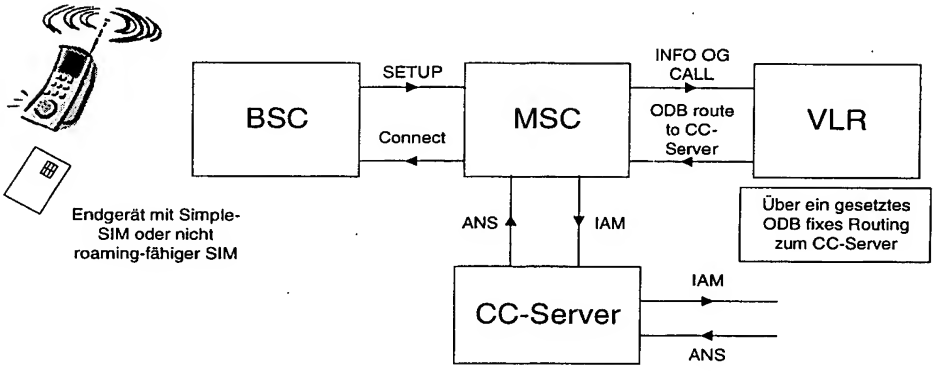



Abbildung 1: Einbuchung ins GSM-Netz mittels Error-Auswertung des HLRs

Rufaufbau über CC-Server




5

Abbildung 2: Identifizierung und Rufaufbau über CC-Server

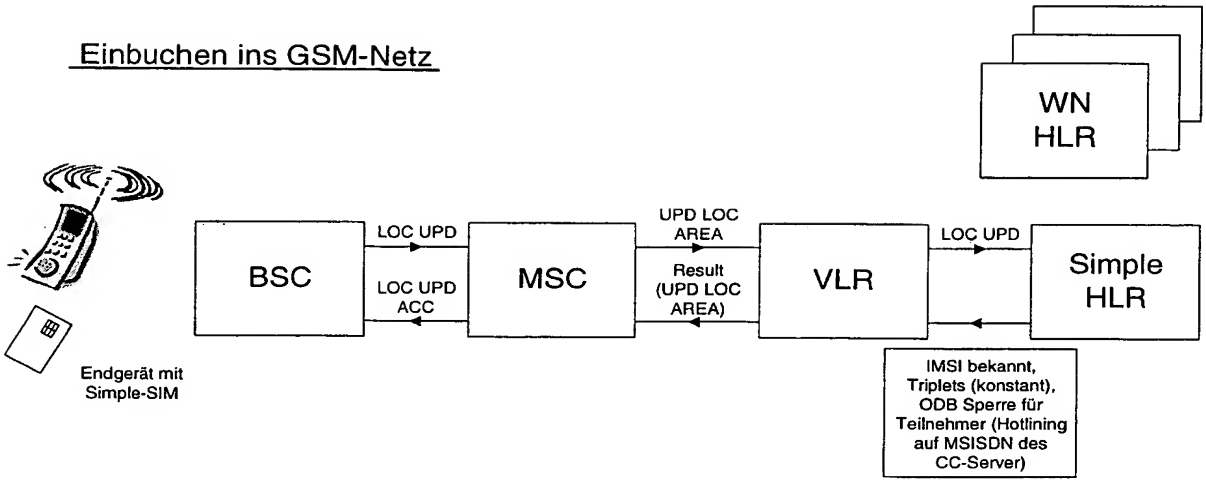



Abbildung 3: Einbuchen ins GSM-Netz mittels Simple-HLR *(nicht Teil der Erfindungsmeldung, weil wahrscheinlich nicht schützenswert - oder?)*

**Neue Geschäftsprozesse**

Das beschriebene Verfahren eröffnet sowohl den Teilnehmern als auch dem Netzbetreiber neue Möglichkeiten bzgl. Dienstenutzung und gegenseitiger Geschäftsbeziehung. Für den Teilnehmer, der in Besitz einer Kreditkarte ist, birgt dieses Verfahren den Vorteil, ohne gültiges (Telekommunikations-)Teilnehmerverhältnis oder ohne gültige Roamingberechtigung dennoch die Dienstleistungen eines Netzbetreibers in Anspruch zu nehmen. Neben der damit verbundenen Umsatzsteigerung hat das Verfahren für den Netzbetreiber jedoch noch einen wesentlichen Vorteil. Die Dienstleistungen, die der Netzbetreiber den (Mobilfunk-)Teilnehmern zur Verfügung stellt, bedürfen keiner Registrierung. Registrierungen heißen für den Netzbetreiber die Bereitstellung entsprechender Systemressourcen, was wiederum sehr kostenintensiv ist. So bindet jede personalisierte SIM, auch wenn sie noch nicht aktiviert ist -

also noch keine MSISDNs und Dienste zugeordnet bekommen hat - Ressourcen in HLR/AC oder im Kartenmanagementsystem KMS. Da diese Ressourcen einerseits teuer sind andererseits auch numerisch begrenzt sind (Nummernbereiche für MSISDN), verbieten sich gewisse Ansätze, wie zum Beipiel eine großzügige Lagerhaltung von SIMs oder das großflächige Verteilen von Karten in die Fläche.

Nicht registrierte SIMs heben diese Restriktionen zum großen Teil auf. So ist es durchaus vorstellbar, sogenannte "Simple-SIMs" in großer Anzahl an Endkunden oder Points of Sales zu verteilen, was ganz andere Vertriebswege eröffnen würde. Unter einer Simple-SIM ist im einfachsten Fall eine Chipkarte zu verstehen, die als einzige Funktionalität die Fähigkeit besitzt, einem Endgerät die Registrierungsprozedur zu ermöglichen, indem es eine IMSI zur Verfügung stellt. Die IMSI muß weder beim Netzbetreiber registriert sein noch muß die Simple-SIM authentisieren können, denn - wie oben beschrieben - fängt der Netzbetreiber diesen "Makel" ab und bietet bei diesen Karten die Registrierung per Kreditkarte an. Das folgende Beipiel zeigt ein mögliches Vertriebsszenario:

- jeder VISA Kunde bekommt mit seiner (VISA-)Monatsrechnung eine Simple SIM zugesandt
- diese SIM ist in einem Handy einsetzbar und erlaubt den (eingeschränkten) Zugang zum D1-Netz, indem die Registrierung über die VISA-Card abgewickelt wird
- die Abrechnung der in Anspruch genommenen Telekommunikationsdienstleistungen erfolgt über die VISA-Card
- entscheidet sich der VISA-Kunde dafür, (im klassischen Sinne) Teilnehmer von D1-zu werden, so schließt er einen

Vertrag mit T-Mobil ab und bekommt eine reguläre D1-SIM zugesandt

Eine Variante dieses Szenarios besteht zum Beispiel darin, die Simple-SIM schon so zu gestalten, dass sie nach der Entscheidung des Kunden, D1-Teilnehmer zu werden, nicht durch eine neue ersetzt werden muß. Dies kann erreicht werden, indem man nachträglich Funktionen auf der SIM aufbringt (over-the air) oder freischaltet, sowie im Netz die Kartendaten in die entsprechenden Systeme einbringt oder freischaltet.

Ein weitere Vertriebsmöglichkeit, welche sich auftut, ist die Nutzung von neuen Vertriebspunkten, die bisher eher ungeeignet sind. Durch den Wegfall der Notwendigkeit, per Vertrag eine Subscription abzuschließen, ist es durchaus vorstellbar, die Simple-SIMs auch in Kioske, Tankstellen, Handelsketten etc. zu geben.

Ebenso bietet es sich an, mit Endgeräteherstellern Agreements zu schließen, so dass diese ihre Endgeräte bereits mit einer Simple-SIM von D1 ausliefern. Dies liegt sowohl im Interesse des Netzbetreibers (selbsterklären) als auch im Interesse des Endgeräteherstellers, dessen Ware bereits ohne Abschluss eines Subscriptionsvertrags telefonierfähig ist.

Eine weitere Zielgruppe wären die bereits bei D1 gebundenen Teilnehmer, die in Besitz eines Zweithandies kommen (z.B. bei Kauf eines Neugeräts und evtl. Abschluss eines Folgevertrags). Ihnen würde die Nutzung des Zweithandies mit einers Simple-SIM weiterhin ermöglicht.

**Patentansprüche**

1. Verfahren zum vereinfachten Zugang zu Telekommunikationsnetzen und Abrechnung von Telekommunikationsdienstleistungen dadurch gekennzeichnet, daß im Netz des Netzbetreibers Authentikationsverfahren eingesetzt werden, mittels derer es dem Teilnehmer ermöglicht wird, zu irgend einem frei wählbaren Zeitpunkt nachzuweisen, dass eine Bezahlung der in Anspruch genommenen oder zu nehmenden Dienstleistung geleistet wird bzw. bereits geleistet wurde.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein Verfahren angewendet wird, mittels dessen die Identität des Benutzers von Dienstleistungen im Telkommunikationsnetz durch mindestens eine der folgenden Maßnahmen durchgeführt wird:

   1) durch eine digitale Signatur;
   2) direkt über bestehende vertrauensvolle Mechanismen (EC-Karte, Elektronische Börse)
   3) zweifelsfrei technisch seine Verbundenheit zu einer vertraulichen, dritten Partei nachweist, die für die Bezahlung einsteht (Kreditkartenorganisation).

3. Anordnung zum vereinfachten Zugang zu Telekommunikationsnetzen und Abrechnung von Telekommunikationsdienstleistungen , dadurch gekennzeichnet, daß Vorrichtungen vorhanden sind, mittels derer der Teilnehmer im zeitlichen Zusammenhang mit einem elektronischen Bezahlvorgang dem Netzbetreiber nachweisen kann, dass eine Bezahlung der in Anspruch genommenen oder zu nehmenden Dienstleistung geleistet wurde bzw. wird.